FY 2014
Chief Information Officer
Federal Information Security Management Act
Micro Agency Reporting Metrics
v1.1

Prepared by:
US Department of Homeland Security
Office of Cybersecurity and Communications
Federal Network Resilience

January 29, 2014

Document History

Version	Date	Comments	Author	Sec/Page
1.0	12/2/13	Initial release of FY14 Micro annual FISMA metrics	D. Waller	All
1.1	1/29/14	Reference change to Section 7	D. Waller	All

NAME: FY 2014 Chief Information Officer Federal Information Security Management Act Micro Agency Reporting Metrics

CREATED: December 2, 2013
AUTHORS: Dominique Waller
BRANCH: Federal Network Resilience
PROGRAM: Cybersecurity Performance Management

Table of Contents

List of Tables

PURPOSE STATEMENT

This document contains the annual security posture questions for FY14. These questions address areas of risk and are designed to assess the implementation of security capabilities and measure their effectiveness.

GENERAL INSTRUCTIONS

Instructions provided below pertain to the entire document. Individual sections may provide instructions specific to that section.

Sources of Questions and Guidance for the United States Government-wide (USG-wide) Federal Information Security Management Act (FISMA) Program

The questions in this document come from three primary sources and will be marked accordingly. In priority order, the sources are the following:

1. Administration Priorities (AP): These questions are determined by the Office of Management and Budget (OMB) and the National Security Staff and will be scored for the following Performance Areas:
    - Continuous Monitoring:
        - Automated Asset Management
        - Automated Configuration Management
        - Automated Vulnerability Management
    - HSPD-12
    - Trust Internet Connections (TIC) v2.0 Capabilities
    - TIC Traffic Consolidation

2. Key FISMA Metrics (KFM): These questions are based on FISMA and will be scored for the following Performance Areas:
    - Privileged User Training
    - Device Discovery Management
    - Remote Access Authentication
    - Remote Access Encryption
    - Domain Name System Security Extensions (DNSSEC) Implementation
    - Controlled Incident Detection

3. Baseline Questions (Base): These questions are derived from National Institute of Standards and Technology (NIST)[1] guidelines and will not be scored. The purpose of baseline questions is to establish current performance, against which future performance may be measured. Some of these questions are also intended to determine whether such future performance measures are needed.

The Federal cybersecurity defensive posture is constantly evolving because of the relentless and dynamic threat environment, emerging technologies, and new vulnerabilities. Many threats can

[1] National Security Systems per FISMA are exempt from NIST standards unless they are included in ICD 503 and referenced in CNSS.

be mitigated by following established cybersecurity best practices, but attackers often search for organizations with poor cybersecurity practices and target associated vulnerabilities. The objective of the AP and KFM metrics is to improve the security posture of Federal Departments/Agencies (D/As) in this ever-changing environment.

Reporting Organizations

This document uses the term "organization" to refer to each Federal D/A that is a reporting unit under CyberScope. Often, those organizations must collect and aggregate their response from a number of subordinate organizational "components." The term "network" refers to a network employed by the organization or one of its divisions to provide services and/or conduct other business. These generic terms are used throughout the document with the understanding that each D/A might use other terms to refer to itself, its networks, and its components.

1. SYSTEM INVENTORY

1.1. For each FIPS 199 impact level (H = High, M = Moderate, L = Low), what is the total number of information systems by organization (i.e., Bureau or Sub-Department Operating Element) categorized at that level?[2] Answer in Table 1. (Organizations with fewer than 5,000 users may report as one unit.)

	1.1.1. Organization-Operated Systems (Base)			1.1.2. Contractor-Operated Systems (Base)			1.1.3. Systems (from 1.1.1 and 1.1.2) with Security ATO (signed, in-scope) (KFM)		
FIPS 199 Category	**H**	**M**	**L**	**H**	**M**	**L**	**H**	**M**	**L**
Reporting Organization 1									
Reporting Organization 2									
[Add rows as needed for organization]									

Table 1— Responses to Questions 1.1.1–1.1.3

[2] Departments and agencies who report systems are expected to follow the Risk Management Framework (RMF), to include guidance on security plans and risk assessments, as outlined in NIST SP 800-37 and NIST SP 800-137.

2. ASSET MANAGEMENT

2.1. What is the total number of the organization's hardware assets connected to the organization's unclassified[3] network(s)?[4] (Base)

2.2. What percentage of assets in 2.1 are covered by an automated capability (scans/device discovery processes) to provide enterprise-level visibility into asset inventory information for all hardware assets? (AP)

2.3. Can the organization track the installed operating system's vendor, product, and version in use on the assets in 2.1? (Base)

2.4. For what number of assets in 2.1 has the organization implemented an automated capability to detect and block unauthorized software from executing or for which no such software exists for the device type?[5] [6] (KFM)

[3] "Unclassified" means low-impact (non-SBU) and SBU networks. Some organizations incorrectly use "unclassified" to mean not classified and not SBU.

[4] Unless specified otherwise in a footnote, add numbers across networks and organizational components to get the reportable result.

[5] This may include software whitelisting tools that identify executable software by a digital fingerprint and selectively block these. It might also include sandboxing of mobile code to determine before execution whether to allow it to run, where static files do not allow whitelisting. In general, any method included should be able to block zero-day and APT threats.

[6] This question is asking for the total percentage for both halves of the conjunctive. For example, if for the assets entered in 2.1, 65% have an automated capability to detect and block unauthorized software from executing and for 20% there is no such software existing, then the response to this question would be 85%.

Definitions for FY2014 Asset Management Section

Automated capability to detect and block unauthorized software from executing
This should be interpreted to include

- anti-virus software (that blocks software based on signatures)
- other black-listing software that is of comparable breadth
- white-listing software that only allows executable software with specific digital fingerprints (or comparable verification method) to execute

In other words, the software may be considered unauthorized if it is on a blacklist or not on a whitelist.

This question refers to capability at the device level, not at the network level. If D/As wish to describe capabilities to filter and block malicious code at the network boundary level, they may do so in the applicable comments section.

Connected to the organization's unclassified network(s)[7]
This includes mechanical (wired), non-mechanical (wireless), and any other form of connection that allows the electronic flow of information. Exclude the following:

- stand-alone devices (not addressable)[8]
- test and/or development networks not connected to the internet and that contain no sensitive information (no information above the low-impact level)
- networks hosting public, non-sensitive websites (no information above the low-impact level) unless access to internal networks can be accomplished by attacking the public website
- classified networks
- Refer to NIST 800-65, Integrating IT Security into the Capital Planning and Investment Control Process, January 2005, for more information.

Hardware assets/components
Organizations have tended to divide these assets into the following categories for internal reporting. (Note: Those that do not meet the criteria defined below should be excluded.) The detailed lists under each broad category are illustrative and not exhaustive. Note that the last category, "other addressable devices on the network," addresses the criterion for including other kinds of specialized devices not explicitly called out.

- non-portable computers[9]
  - servers

[7] There is no limit on the connection (low frequency or low duration). Even short and/or infrequent connections should be counted. Regardless of how much or little these connected devices are intended to process, store, and transmit information, once connected they can be abused for misuse of the network.
[8] This should not be interpreted to exclude devices that are intermittently connected, which should be included.
[9] A multi-purpose device needs to be counted only once. A device with multiple IP connections needs to be counted only once, not once per connection. This is an inventory of hardware assets, not data.

    - workstations (desktops)
- portable computers
    - laptops
    - net-books
    - tablets (iPad, Kindle, other Android)
- mobile devices
    - smartphones (iPhone, Android)
    - cell phones
    - BlackBerry
- networking devices[10]
    - routers
    - switches
    - gateways, bridges, wireless access points (WAPs)
    - firewalls
    - intrusion detection/prevention systems
    - network address translators (NAT devices)
    - hybrids of these types (e.g., NAT router)
    - load balancers
    - modems
- other communication devices
    - encryptors
    - decryptors
    - VPN endpoints[11]
    - medical devices that are part of a patient monitoring network
    - alarms and physical access control devices
    - PKI infrastructure[12]
- Other input/output devices if they appear with their own address
    - network printers/plotters/copiers/multi-function devices (MFDs)
    - network fax portals
    - network scanners
    - network accessible storage devices
    - VOIP phones
    - others network I/O devices
- Virtual machines that can be addressed[13] as if they are a separate physical machine should be counted as separate assets,[14] including dynamic and on-demand virtual environments.

[10] This list is not meant to be exhaustive, as there are many types of networking devices. If they are connected, they are to be included.
[11] "VPN endpoints" generally means the encryptors/decryptors at each end of the VPN tunnel.
[12] PKI assets should be included in the network(s) on which they reside. Special methods may be needed to adequately check them for vulnerabilities, compliance, etc. as described in subsequent sections. If this is not done, PKI assets should be included among the assets not covered.
[13] "Addressable" means by IP address or any other method to communicate to the network.

- other devices addressable on the network
- USB devices connected to any device addressable on the network

Both Government Furnished Equipment (GFE) assets and non-GFE assets are included if they meet the other criteria for inclusion listed here.[15] Mobile devices that receive Federal email are considered to be connected. Note: If a non-GFE asset is allowed to connect, it is especially important that it be inventoried, authorized, and correctly configured prior to connection.[16]

Only devices connected to the network(s) of the organization should be reported, and only if they are addressable[17] for network traffic (except USB-connected devices, which are included). We limit this definition to addressable devices because, from a network point of view, only addressable devices are attackable. For example, a monitor (not addressable, thus not included) can be attacked only through the addressable computer it is connected to. Connected USB devices are included because they are a source of attacks.

Visibility at the organization's enterprise level

The information about hardware assets can be viewed at one of two levels:

- the whole reporting organization
- the lower levels of the organization, as long as they are operated as semi-independent units and are large enough to provide reasonable economies of scale while remaining manageable. (Organizations should consult with DHS/FNR on the appropriateness of the definition of lower levels of the organization, if in doubt.)

[14] Note that VM "devices" generally reside on hardware server(s). Assuming that both the hardware server and the VM server are addressable on the network, both kinds of devices are counted in the inventory, because each needs to be managed and each is open to attack. (Things like multiple CPUs, on the other hand, do not create separate assets, generally, because the CPUs are not addressable and are subject to attack only as part of the larger asset). If you have issues about how to apply this for specific cloud providers, please contact FedRAMP for further guidance: http://www.gsa.gov/portal/category/102371.

[15] If a non-GFE asset connects in a limited way such that it can only send and receive presentation-layer data from a virtual machine on the network, and this data has appropriate encryption (such as a Citrix connection), it does not have to be counted.

[16] If a non-GFE connects in a limited way such that it can only send and receive presentation-layer data from a virtual machine on the network, and this data has appropriate encryption (such as a Citrix connection), it does not have to be counted.

[17] "Addressable" means that communications can be routed to this asset, typically because it has an assigned IP address. Devices connecting via mechanisms like Citrix where only limited traffic can be allowed to pass do not need to be counted if justified by an adequate risk assessment, approved by the AO.

3. CONFIGURATION MANAGEMENT

3.1. For each operating system, vendor, product, and version referenced in 2.3, report the following:

Vendor/Operating System/Version	3.1.1. Has a minimal acceptable security configuration baseline been defined? [18] (KFM)	3.1.2. How many hardware assets (which are covered by this baseline, if it exists) have this software? (KFM)	3.1.3. What is the percentage of the applicable hardware assets (per question 2.1) of each kind of operating system software in 3.1 covered by an automated capability to identify deviations from the approved configuration baselines identified in 3.1.1 and to provide visibility at the organization's enterprise level? (AP)

[18] "Defined" may include a narrative definition of the desired configuration. In the future, we will expect these standards to be defined directly as (a) data or (b) a test (preferably automated) of the configuration. Consider an organization approved deviation as *part* of the organization standard security configuration baseline.

Definitions for FY2014 Configuration Management Section

Applicable hardware assets

Those hardware assets counted in section 2.1 on which the software in question is installed and configured.

Automated capability to identify configuration deviations from the approved baselines

Any report of assets that can be generated by a computer. This includes

- active configuration scanners
- agents on devices that report configuration
- reports from software that can self-report its configuration
- running a script to retrieve data
- any other reliable and valid method
- some combination of the above

Organization approved deviation[19]

This shall be interpreted to include deviations approved for

- specific devices or classes of devices
- specific classes of users
- specific combinations of operating system and/or applications
- other purposes to meet business needs

Such deviations should generally be supported by a risk-based analysis,[20] which justifies any increased risk of the deviation based on business needs. The deviation must be approved in accordance with organizational policies and procedures.

[19] Organizations that adopt generic standard configurations without deviation should be perfectly free to do so, as long as those configurations were developed by a source that adequately addressed security (NSA, NIST, DISA, CIS, etc.).

[20] This should not be interpreted as a requirement for overly extensive documentation of these risk-based analyses, but rather for just enough to allow the system owner and AO to make an informed decision.

4. VULNERABILITY AND WEAKNESS MANAGEMENT

4.1. What percentage of hardware assets identified in section 2.1 are evaluated using an automated capability that identifies NIST National Vulnerability Database vulnerabilities (CVEs) present with visibility at the organization's enterprise level? (AP)[21]

Definitions for FY2014 Vulnerability and Weakness Management Section

Automated capability to identify vulnerabilities

Any report of actual assets that can be generated by a computer. This includes

- active vulnerability scanners
- agents on devices that report vulnerabilities
- reports from software that can self-report its version and patch level, which is then used to identify vulnerabilities from NVD that are applicable to that version and patch level
- any other reliable and valid method
- some combination of the above

[21] Once all organizations are reporting monthly to CyberScope, this question may become redundant.

5. IDENTITY AND ACCESS MANAGEMENT

5.1. How many people have unprivileged network[22] accounts? (Exclude privileged network accounts and non-user accounts.) (Base)

5.2. What percentage of people with an *unprivileged* network account can log onto the network in each of the following ways? See Table 2.

Metric	Percentage [23]	Comments
5.2.1. Allowed to log on with user ID and password. (Base)		Measures the percentage of people who are allowed to use user ID and password as their normal mode of authentication. • Percentage should measure people because a person may have multiple accounts. • For a person with more than one unprivileged network account, the person should be counted in the percentage if the person is permitted to use user ID and password to log onto any account.
5.2.2. Allowed, but not required, to log on with a non-PIV form of two-factor authentication. (Base)		Measures the percentage of people whose accounts have been enabled to allow logon using a non-PIV form of two-factor authentication. • Percentage may include an account that allows both non-PIV, two-factor authentication and an alternative authentication mechanism (such as user ID and password). • Percentage should measure people because a person may have multiple accounts. • For a person with more than one unprivileged network account, the person should be counted in the percentage if the person is permitted to use a non-PIV form of two-factor authentication to log onto any account.

[22] An unprivileged network account is an account without elevated privileges.
[23] Each row should be assessed independently; the percentages are not expected to sum to 100%.

Metric	Percentage [23]	Comments
5.2.3. Allowed, but not required, to log on with a two-factor PIV card. (Base)		Measures the percentage of people whose accounts have been enabled to allow logon using a two-factor PIV card. • Percentage may include an account that allows both PIV and an alternative authentication mechanism (such as user ID and password). • Percentage should measure people because a person may have multiple accounts. • For a person with more than one unprivileged network account, the person should be counted in the percentage if the person is permitted to use a two-factor PIV card to log onto any account.
5.2.4. Required to log on with a non-PIV form of two-factor authentication. (Base)		Measures the percentage of people who are required to log on using a non-PIV form of two-factor authentication as the normal mode of authentication. • Percentage should measure people because a person may have multiple accounts. • For a person with more than one unprivileged network account, the person should be counted in the percentage only if the person is required to use two-factor authentication for all accounts.[24]

[24] Organizations are expected to transition all network access to two-factor PIV card authentication; therefore, this metric should not be construed as requiring implementation of alternative non-PIV forms of two-factor authentication. During the transition to two-factor PIV card authentication, this metric is expected to include people who are required to use PIV card authentication on some accounts and non-PIV two-factor authentication on other accounts who have not yet been transitioned or cannot be transitioned to PIV card authentication due to the technical limitations of the implementation.

Metric	Percentage [23]	Comments
5.2.5. Required to log on with a two-factor PIV card. (AP)[25]		Measures the percentage of people who are required to log on using a two-factor PIV card as the normal mode of authentication. Question 5.2.5 is inclusive of anyone counted in 5.2.6. • Percentage should include people currently using temporary credentials if the person's normal mode of authentication is PIV-enforced. • Percentage should measure people because a person may have multiple accounts. • For a person with more than one unprivileged network account, the person should be counted in the percentage only if the person is required to use a two-factor PIV card to authenticate to all accounts.
5.2.6. Required to conduct PIV authentication at the user-account level. (KFM)[26]		Measures the percentage of people for whom only the PIV card can be used to log onto the person's account. • Percentage should measure people because a person may have multiple accounts. • For a person with more than one unprivileged network account, the person should be counted in the percentage only if two-factor PIV card authentication is enforced at the user-account level for all accounts.

Table 2 – Responses to Questions 5.2.1–5.2.6

5.3. How many people have privileged network accounts? (Exclude unprivileged network accounts and non-user accounts.) (Base)

[25] When reporting how many PIV credentials are being used for logical access to systems, agencies should include the following implementations: Remote or networked logical access system implementations are PIV -enabled when the Public Key Infrastructure (PKI) certificate presented at authentication is validated (Le., found to be legitimately issued, unexpired, and unrevoked) under Federal Common Policy as a PIV Authentication Certificate and the corresponding "PIV Authentication Key" on the card correctly responds to the cryptographic challenge in the authentication protocol to gain access. Certificate validation may be performed by an intermediary service such as a Server-based Certificate Validation Protocol (SCVP) server. Revocation checking may be accomplished by 'caching' revocation information from the credential issuer provided the cache is refreshed at least once every 18 hours. Local workstation logical access system implementations are PIV -enabled when the BIO, BIO-A, CHUID, or PIV Authentication credentials and authentication protocols are in conformance with authentication mechanisms defined in FIPS 201 and NIST SP 800-73, digital signatures on data objects used are verified, and certificates used are validated. System implementations protected by an Identity and Access Management solution that adheres to the principles above are also considered PIV -enabled. For additional information, refer to FIPS 201, NIST SP 800-73, and Federal PKI Policy and FICAM Roadmap and Implementation Guidance.

[26] This metric is operating-system specific and is intended to assess a specific implementation method. It may not apply to all operating system platforms.

5.4. What percentage of people with a *privileged* network account can log onto the network in each of the following ways? See Table 3.

Metric	Percentage[27]	Comments
5.4.1. Allowed to log on with user ID and password. (Base)		Measures the percentage of people who are allowed to use user ID and password as their normal mode of authentication. • Percentage should measure people because a person may have multiple accounts. • For a person with more than one privileged network account, the person should be counted in the percentage if the person is permitted to use user ID and password to log onto any account.
5.4.2. Allowed, but not required, to log on with a non-PIV form of two-factor authentication. (Base)		Measures the percentage of people whose accounts have been enabled to allow logon using a non-PIV form of two-factor authentication. • Percentage may include an account that allows both non-PIV two-factor authentication and an alternative authentication mechanism (such as user ID and password). • Percentage should measure people because a person may have multiple accounts. • For a person with more than one privileged network account, the person should be counted in the percentage if the person is permitted to use a non-PIV form of two-factor authentication to log onto any account.
5.4.3. Allowed, but not required, to log on with a two-factor PIV card. (Base)		Measures the percentage of people whose accounts have been enabled to allow logon using a two-factor PIV card. • Percentage may include an account that allows both PIV and an alternative authentication mechanism (such as user ID and password). • Percentage should measure people because a person may have multiple accounts. • For a person with more than one privileged network account, the person should be counted in the percentage if the person is permitted to use a two-factor PIV card to log onto any account.

[27] Each row should be assessed independently; the percentages are not expected to sum to 100%.

Metric	Percentage[27]	Comments
5.4.4. Required to log on with a non-PIV form of two-factor authentication. (Base)		Measures the percentage of people who are required to log on using a non-PIV form of two-factor authentication as the normal mode of authentication. • Percentage should measure people because a person may have multiple accounts. • For a person with more than one privileged network account, the person should be counted in the percentage only if the person is required to use two-factor authentication for all accounts.[28]
5.4.5. Required to log on with a two-factor PIV card. (AP)		Measures the percentage of people who are required to log on using a two-factor PIV card as the normal mode of authentication. Question 5.4.5 is inclusive of anyone counted in 5.4.6. • Percentage should include people currently using temporary credentials if the person's normal mode of authentication is PIV-enforced. • Percentage should measure people because a person may have multiple accounts. • For a person with more than one privileged network account, the person should be counted in the percentage only if the person is required to use a two-factor PIV card to authenticate to all accounts.
5.4.6. Required to conduct PIV authentication at the user-account level. (KFM)[29]		Measures the percentage of people for whom only the PIV card can be used to log onto the person's account. • Percentage should measure people because a person may have multiple accounts. • For a person with more than one privileged network account, the person should be counted in the percentage only if two-factor PIV card authentication is enforced at the user-account level for all accounts.

Table 3 – Responses to Questions 5.4.1–5.4.6

[28] Organizations are expected to transition all network access to two-factor PIV card authentication; therefore, this metric should not be construed as requiring implementation of alternative non-PIV forms of two-factor authentication. During the transition to two-factor PIV card authentication, this metric is expected to include people who are required to use PIV card authentication on some accounts and non-PIV two-factor authentication on other accounts who have not yet been transitioned or cannot be transitioned to PIV card authentication due to the technical limitations of the implementation.

[29] This metric is operating-system specific and is intended for a specific implementation. It may not be applicable to all operating system platforms. Organizations are not required or expected to adopt the authentication method described in the metric, organizations that record 0% in this column will not be penalized.

This section applies to remote access solutions that protect access to the organization's desktop LAN/WAN resources and services. Remote access excludes externally facing applications (e.g., OWA).

5.5. How many people log onto the organization's remote access solution(s) to obtain access to the organization's desktop LAN/WAN resources or services? (Base)

5.6. Of the people reported in 5.5, how many can remotely log onto the organization's desktop LAN/WAN resources or services in each of the following ways? See Table 4.

Metric	Percentage[30]	Comments
5.6.1. Allowed to log on with user ID and password. (Base)		Measures the percentage of people who are allowed to use user ID and password as their normal mode of authentication for remote access. • Percentage should measure people because a person may have multiple accounts. • People with more than one account should be counted in the percentage if they are permitted to use user ID and password to log onto any account.
5.6.2. Allowed, but not required, to log on with a non-PIV form of two-factor authentication. (Base)		Measures the percentage of people who are allowed to log on using a non-PIV form of two-factor authentication for remote access. • Percentage may include an account that allows both non-PIV two-factor authentication and an alternative authentication mechanism (such as user ID and password). • Percentage should measure people because a person may have multiple accounts. • People with more than one account should be counted in the percentage if they are permitted to use a non-PIV form of two-factor authentication to log onto any account.
5.6.3. Allowed, but not required, to log on with a two-factor PIV card. (Base)		Measures the percentage of people who are allowed to log on using a two-factor PIV card for remote access. • Percentage may include an account that allows both PIV and an alternative authentication mechanism (such as user ID and password). • Percentage should measure people because a person may have multiple accounts. • People with more than one account should be counted in the percentage if they are permitted to use a two-factor PIV card to log onto any account.

[30] Each row should be assessed independently; the percentages are not expected to sum to 100%.

Metric	Percentage[30]	Comments
5.6.4. Required to log on with a non-PIV form of two-factor authentication. (Base)		Measures the percentage of people who are required to log on using a non-PIV form of two-factor authentication as the normal mode of authentication for remote access. • Percentage should measure people because a person may have multiple accounts. • People with more than one account should be counted in the percentage only if they are required to use two-factor authentication for all accounts.[31]
5.6.5. Required to log on with a two-factor PIV card. (KFM)		Measures the percentage of people who are required to log on using a two-factor PIV card as the normal mode of authentication for remote access. Question 5.6.5 is inclusive of anyone counted in 5.6.6. • Percentage should include people currently using temporary credentials if the person's normal mode of authentication is PIV-enforced. • Percentage should measure people because a person may have multiple accounts. • People with more than one account should be counted in the percentage only if they are required to use a two-factor PIV card to authenticate to all accounts.
5.6.6. Required to conduct PIV authentication at the user-account level. (KFM)[32]		Measures the percentage of people for whom only the PIV card can be used to log onto the person's account for remote access. • Percentage should measure people because a person may have multiple accounts. • People with more than one account should be counted in the percentage only if two-factor PIV card authentication is enforced at the user-account level for all their accounts.

Table 4 – Responses to Questions 5.6.1 to 5.6.6

[31] Organizations are expected to transition all network access to two-factor PIV card authentication; therefore, this metric should not be construed as requiring implementation of alternative non-PIV forms of two-factor authentication. During the transition to two-factor PIV card authentication, this metric is expected to include people who are required to use PIV card authentication on some accounts and non-PIV two-factor authentication on other accounts that have not yet been transitioned or cannot be transitioned to PIV card authentication due to the technical limitations of the implementation.

[32] This metric is operating-system specific and is intended to assess a specific implementation method. It may not apply to all operating system platforms.

Definitions for FY2014 Identity and Access Management Section

Allow a specific form of identification

The specific form of identification (credential) listed in the question may be used for authentication, but this form is not required because at least one other type of credential may also be used. (In this case, the form of authentication chosen may affect privileges to some degree.) Contrast with "require a specific form of identification."

Network account

Account defined on the network, rather than on a local machine. It is assumed that network accounts are the primary type used, and that local (machine) accounts are accessed primarily through network-level accounts and credentials.

Network accounts with elevated privileges

A network account that provides access to powers and data within the system/application that is significantly greater than those available to the majority of accounts. Also known as "privileged network user accounts." Such greater powers include, but are not limited to, the ability to

- view/copy/modify/delete sensitive system meta-information[33] and/or network resources
- change the access rights to network resources

At a low level of privilege, the account with elevated privileges may only be able to perform limited privileged functions on a subset of objects on the network. At the other extreme, the user account with elevated privileges may have full control of all objects on the network. The risk (impact) of compromise is greater because the account has more privileges.

Accounts with elevated privileges are typically allocated to system administrators, network administrators, DBAs, and others who are responsible for system/application control, monitoring, or administration functions. (Exclude system and application accounts utilized by processes because they are non-user accounts, and exclude local workstation administrators because they are not network accounts.)

Network accounts without elevated privileges

Any network account that is not a network account with elevated privileges. Also known as "unprivileged network accounts."

[33] System meta-information means the information used to configure the network, a device, an operating system or application on the device, a user-account, a policy object, an executable file, etc. In general it does not include the ability to view/copy/modify/delete the documents and transactions necessary for a person to perform a normal business function. But it does include "super-users" of a business application who have broad rights to view/copy/modify/delete the transactions of multiple other users.

Non-user account
An account that is not intended to be controlled directly by a person (or group). The account is either (a) intended to be used by the system or an application, which presents credentials and performs functions under the management of the person (or group) that owns the account[34] or (b) created to establish a service (like a group mailbox), and no one is expected to log into the account. Non-user accounts are typically called group mailbox, service, and/or system accounts.[35]

Other two-factor authentication
Some other form of two-factor authentication (e.g., not involving a PIV card), for example, a user ID and password combined with a random token generator (for example; an RSA key fob).

PIV credentials
A PIV card (credential) is a "Personal Identity Verification Card" as defined in NIST FIPS 201. For the purposes of answering this question, we count only cards that use three-factor authentication. Typically the card is read through a reader that takes a security certificate from the PIV card. The same user will then be identified by some other factor. DOD Common Access Cards (CAC Cards) are included in this category for DOD organizations.

Privileged network user
A privileged network user is a user who, by virtue of function and/or seniority, has been allocated a network user account with elevated privileges. Such persons include, for example, the system administrator(s) and network administrator(s) who are responsible for keeping the system available and may need powers to create new user profiles as well as add to or amend the powers and access rights of existing users.[36]

Require a specific form of identification
Only this specific form of identification (credential) may be used for authentication. Contrast with "allow a specific form of identification."

User accounts
An account that is intended to be controlled directly by a particular person to perform work. The person presents their credential to gain access. User accounts include temporary, guest, and generic student accounts.

User ID and password
User ID and password is the traditional credential used on most networks. The user ID is public, and the password is private, so this is considered to be one-factor authentication.

[34] For example, this includes machine accounts and operating system built-in accounts. More generally, it includes "service" accounts.
[35] This does not include maintenance provider accounts, where the user is a person, nor does it include cloud provider system administrators. Those accounts are to be included in user accounts.
[36] http://www.yourwindow.to/information-security/gl_privilegeduser.htm

6. DATA PROTECTION

Purpose and Use

6.1. What is the estimated number of hardware assets from 2.1 in each of the following mobile asset types, and how many are encrypted? Answer in Table 5. (KFM)

Mobile Asset Types (each asset should be recorded *no more than once* in each column)	**a. Estimated number of mobile hardware assets of the types indicated in each row.**	**b. Estimated number of assets from column *a* with encryption of data on the device.[37]**
Laptop computers and netbooks		
Tablet-type computers		
BlackBerries and other smartphones		
USB-connected devices (e.g., flash drives and removable hard drives)		
Other mobile hardware assets (describe types in comments field)		

Table 5 – Responses to Question 6.1

Definitions for FY2014 Data Protection Section

BlackBerry
A brand of smartphone provided by the Canadian firm Research in Motion (RIM).

Encryption
All user data is encrypted with FIPS 140-2-validated cryptographic modules, or modules approved for classified data. If the device is not allowed to contain sensitive but unclassified information, count it as adequately encrypted.

Estimated total number
While it would be better if the organization could accurately count all mobile assets, this may not be feasible for all asset types. The intent is that the organization should know the number of mobile assets with sufficient accuracy to be able to measure year-to-year progress on managing encryption and other controls. Thus, these estimates should be less than an order of magnitude more accurate than the expected rate of improvement. If the organization made a very small amount of improvement, or cannot tell whether it made improvement from year to year because of the inability to count these assets, then this should be indicated in the comments.

[37] The numbers in column *b* cannot be larger than the numbers in column *a*.

FIPS 140-2
FIPS 140-2 is a Federal Information Processing Standard that specifies the security requirements satisfied by a cryptographic module utilized within a system. While many vendors claim their cryptographic modules are FIPS 140-2 compliant, only those currently validated as compliant can be reliably counted in this report. (Validation is provided through independent laboratories via the Cryptographic Module Validation Process managed by NIST. See http://csrc.nist.gov/groups/STM/cmvp/index.html for more information on this process and a listing of validated cryptographic modules.)

Flash drives
A solid-state drive (SSD), sometimes called a solid-state disk or electronic disk. An SSD is a data storage device that uses solid-state memory to store persistent data with the intention of providing access in the same manner as a traditional block I/O hard disk drive. These may connect through a USB port or may be plugged directly into devices like smartphones. In either case, flash drives can leave data in a highly vulnerable state.

Laptop computer
A computer intended to be carried by the user and used in a wide variety of environments, including public spaces.

Mobile hardware assets
A hardware asset (typically holding data, software, and computing capability) designed to be used in a wide variety of environments, including public spaces, and/or connected to a number of different networks. These often have wireless capability requiring special controls.

Netbook
A small, lightweight, and inexpensive laptop computer. Netbooks typically lack an internal CD/DVD drive, legacy ports, an ISA bus, or sometimes any internal expansion bus at all.

Removable hard drives
Hard drives that are usually connected to the computer through USB ports, reside externally to the computer, and allow easy removal and connection to other computers. This category could also include similar drives connected directly to the network that allow easy removal and connection to other networks.

Smartphone
A high-end mobile phone built on a mobile computing platform, with more advanced computing ability and connectivity than a contemporary feature phone.

Tablet computer
A mobile computer, larger than a mobile phone or personal digital assistant, integrated into a flat touch-screen and primarily operated by touching the screen rather than using a physical keyboard and mouse. Tablets often use an onscreen virtual keyboard, a passive stylus pen, or a digital pen.

7. BOUNDARY PROTECTION

Instruction: Questions 7.1–7.2 apply only to Federal civilian organizations. If the reporting organization is not a Federal civilian organization, answer N/A to these questions.

7.1. What percentage of external network traffic to/from the organization's networks passes through a TIC/MTIPS? (AP)

7.2. What percentage of external network/application interconnections to/from the organization's networks passes through a TIC/MTIPS? (KFM)

Instruction: The remaining questions apply to all reporting organizations.

7.3. What percentage of organization email systems implement sender verification (anti-spoofing) technologies when sending messages? (KFM)

7.4. What percentage of organization email systems use sender verification (anti-spoofing) technologies to detect possibly forged messages from outside the network? (KFM)

Definitions for FY2014 Boundary Protection Section

Email systems
Organizational software such as Outlook Exchange or Gmail that provides email accounts that enable people to exchange digital messages.

Sender verification (anti-spoofing) technologies
These include

- Domain Keys Identified Mail (DKIM)
- Sender Policy Framework (SPF)
- digital signing of email using PKI
- other technologies able to prevent spoofing (described in the comments)

TIC 2.0 capabilities
A body of 60 critical capabilities that were collaboratively developed to improve upon the baseline security requirements in TIC Reference Architecture V2.0. These are available on OMB's MAX Portal.

TIC/MTIPS (trusted internet connections/managed trusted internet protocol services)
A GSA program described by both **DHS** and **GSA**.

8. TRAINING AND EDUCATION

8.1. What percentage of the organization's network users were given and successfully completed cybersecurity awareness training in the past year (at least annually)? (KFM)

8.1.1. What is the estimated percentage of new users who satisfactorily completed security awareness training before being granted network access, or completed security awareness training within an organizationally defined time limit that provides minimal acceptable security after being granted access? (KFM)

Definitions for FY2014 Training and Education Section

Given and successfully completed cybersecurity awareness training

For situations that are likely[38] to confront unprivileged network users, users have received training that gives them the ability to

- avoid behaviors that would compromise cybersecurity
- practice good behaviors that will increase cybersecurity
- act wisely and cautiously, where judgment is needed, to increase cybersecurity

Successful completion means (at a minimum) that the user has passed a test on the content. Preferably, it means that the user's behavior and judgment is measurably adequate to protect security.

Note that such training may be provided via (a) periodic awareness training spread over the year, (b) an annual course, and/or (c) a combination of annual and more frequent training.

Given that the objective of this training is to affect behavior, training about concepts that are not

Network user

Any person who has access to an unprivileged or privileged network account (as defined in Section 5) on any one (or more) of the organization's networks.

[38] "Likely" is used here to indicate that organizations should use risk-based analysis to decide what behaviors should be covered in this awareness training. Organizations are expected to conduct risk-based analyses to determine the right level of training needed to most cost effectively improve security based on identifying the behaviors that have the most impact given current organizational experience, threats, and countermeasures.

Appendix A: Computing the Administration Priority Metrics

This appendix describes how the FY14 quarterly and annual FISMA metrics as reported to CyberScope are computed to derive a government-wide average for each capability area of the Administration's priorities. The government-wide averages are computed from the FISMA submissions of the 24 Chief Financial Officers (CFO) Act agencies. Beyond FY12, as the metrics are refined, more complex algorithms or weighting may become part of the calculations.

Overall CAP Score—The overall Cross Agency Priority (CAP) score is currently weighted as the average of the three Continuous Monitoring scores plus the TIC score plus the PIV score. All capabilities are considered equally important. Future overall CAP scores may reflect a different weighting because an individual capability might increase in priority.

Continuous Monitoring—The continuous monitoring score is the average of the following three components of continuous monitoring:

> **Asset Management**—Organizations are asked for the total number of organization information technology hardware assets. They are then asked to report the number of these organization assets for which an automated process provides enterprise-level visibility into asset inventory information. The responses from the 24 CFO Act agencies are totaled for hardware assets (*a*) and assets under the automated asset process (*b*). Dividing the total number of hardware assets with automated asset inventory information by the total number of hardware assets (*b*/*a*) gives a government-wide percentage of automated asset management.
>
> **Configuration Management**—Organizations are asked for the number of assets for which an automated process provides enterprise-level visibility into system configuration information to identify deviations from approved configuration baselines. The responses for the 24 CFO Act agencies are totaled for assets with an automated configuration process (*c*). Dividing the total number of hardware assets with automated configuration information by the total number of hardware assets (*c*/*a*) gives a government-wide percentage of automated configuration management.
>
> **Vulnerability Management**—Organizations are asked for the number of assets for which an automated process provides enterprise-level visibility into NIST National Vulnerability Database vulnerabilities (CVEs). The responses for the 24 CFO Act agencies are totaled for assets with an automated vulnerability process (*d*). Dividing the total number of hardware assets with automated vulnerability information by the total number of hardware assets (*d*/*a*) gives a government-wide percentage of automated vulnerability management.

PIV—The FY14 CAP percentage for PIV-required authentication is obtained by dividing the total number of unprivileged and privileged people who are required to log onto the network

using two-factor PIV cards by the total number of unprivileged and privileged access people who are allowed to log onto the network.

To determine the number of people with an unprivileged network account who are required to use PIV, multiply the percentage in 5.2.5 by the total in 5.1.

> *5.2.5. [What percentage of people with an unprivileged network account] are required to log on with a two-factor PIV card? (AP)*
>
> *5.1. How many people have unprivileged network accounts? (Exclude privileged network accounts and non-user accounts.) (Base)*

To determine the number of people with a privileged network account who are required to use PIV, multiply the percentage in 5.4.5 by the total in 5.3.

> *5.4.5. [What percentage of people with a privileged network account] are required to log on with a two-factor PIV card? (AP)*
>
> *5.3. How many people have privileged network accounts? (Exclude unprivileged network accounts and non-user accounts.)(Base)*

To determine the total number of people who are required to log on using two-factor PIV cards, sum the results of the two calculations above.

The sum of 5.1 plus 5.3 equals the number of people with either an interactive or remote network logon account.

The calculation of the FY14 CAP percentage for PIV-required authentication is as follows:

$$\frac{\big((5.1) * (5.2.5)\big) + ((5.3) * (5.4.5))}{(5.1) + (5.3)}$$

TIC capabilities—Organizations report quarterly on the percentage of the required TIC 2.0 capabilities that are implemented. These self-reported numbers are then used to compute a government average for the large CFO Act agencies. The percentages for the CFO Act agencies are totaled and divided by 23 (DOD is exempted from reporting).

TIC consolidation—Organizations report quarterly on the percentage of external network traffic passing through a TIC/MTIPS. These self-reported numbers are then used to compute a government average for the large CFO Act agencies. The percentages for the CFO Act agencies are totaled and divided by 23 (DOD is exempted from reporting).

Recap

Automated Asset Management =

$$\frac{number\ of\ CFO\ Act\ agency\ assets\ under\ enterprise-level\ automated\ asset\ inventory\ process}{total\ number\ of\ hardware\ assets\ across\ the\ 24\ CFO\ Act\ agencies}$$

Automated Configuration Management =

$$\frac{number\ of\ CFO\ Act\ agency\ assets\ under\ enterprise-level\ automated\ configuration\ process}{total\ number\ of\ hardware\ assets\ across\ the\ 24\ CFO\ Act\ agencies}$$

Automated Vulnerability Management =

$$\frac{number\ of\ CFO\ Act\ agency\ assets\ under\ enterprise-level\ automated\ vulnerability\ process}{total\ number\ of\ hardware\ assets\ across\ the\ 24\ CFO\ Act\ agencies}$$

PIV =

$$\frac{number\ of\ CFO\ Act\ agency\ user\ accounts\ configured\ to\ require\ PIV\ card\ for\ access\ to\ agency\ networks}{total\ number\ of\ user\ accounts\ for\ the\ 24\ CFO\ Act\ agencies}$$

TIC capabilities =

$$\frac{total\ of\ CFO\ Act\ agency\ reported\ percentages\ for\ TIC\ capabilities\ implemented}{23}$$

TIC consolidation=

$$\frac{total\ of\ CFO\ Act\ agency\ reported\ percentages\ for\ TIC\ traffic\ consolidation}{23}$$

Appendix B: Acronyms

AO	Authorizing Official
AP	Administration Priorities
APT	Advanced Persistent Threat
ATO	Authorization to Operate
BASE	Baseline Questions
BYOD	Bring Your Own Device
CA	Certificate Authority and/or Certification Authority
CAC	Common Access Cards
CAPEC	Common Attack Pattern Enumeration and Classification
CCB	Configuration Control Board
CCE	Common Configuration Enumeration
CIO	Chief Information Officer
CIS	Center for Internet Security
CM	Continuous Monitoring
CMWG	Continuous Monitoring Working Group
COCO	Contractor Owned Contractor Operated
COTS	Commercial Off The Shelf
CPE	Common Product Enumeration.
CPU	Central Processing Unit
CVE	Common Vulnerabilities and Exposures
CVSS	Common Vulnerability Scoring System
CWE	Common Weakness Enumeration
CWSS	Common Weakness Scoring System
D/A	Department/Agency
DBA	Database Administrator
DHS	Department of Homeland Security
DISA	Defense Information Systems Agency
DKIM	Domain Keys Identified Mail
DLP	Data Loss Protection
DMZ	Demilitarized Zone
DNS	Domain Name System
DNSSEC	Domain Name System Security Extension
DRM	Digital Rights Management
FAQ	Frequently Asked Questions
FDCC/USGCB	Federal Desktop Core Configuration / United States Government Configuration Baseline
FedRAMP	Federal Risk and Authorization Management Program

FICAM	Federal Identity Credential and Access Management
FIPS	Federal Information Processing Standards
FNS	Federal Network Security
FPKIPA	Federal Public Key Infrastructure Policy Authority
GFE	Government Furnished Equipment
GOCO	Government Owned Contractor Operated
GOGO	Government Owned Government Operated
GOTS	Government Off the Shelf
HSPD	Homeland Security Presidential Directive
HW	Hardware
I/O	Input/Output
IP	Internet Protocol
ISP	Internet Service Provider
KFM	Key FISMA Metrics
LAN	Local Area Network
MAC	Media Access Control
MAC	Media Access Card
MAN	Metropolitan Area Network
MFD	Multi-Function Device
MTIPS	Managed Trusted Internet Protocol Services
NAC	Network Access Controls
NAT	Network Address Translators
NIST	National Institute of Standards and Technology
NIST SP	National Institute of Standards and Technology Special Publication
NOC	Network Operations Center
NSA	National Security Agency
NVD	National Vulnerability Database
OIG	Office of the Inspector General
OMB	Office of Management and Budget
OPM EHRI	Office of Personnel Management Enterprise Human Resources Integration
OS	Operating System
OVAL	Open Vulnerability and Assessment Language
OWA	Outlook Web Access
PGP	Pretty Good Privacy
PII	Personally Identifiable Information
PIV	Personal Identity Verification
PKI	Public Key Infrastructure
RA	Registration Authority
S/MIME	Secure/Multipurpose Internet Mail Extensions

SAR	Security Awareness Reports
SBU	Sensitive but Unclassified
SCAP	Secure Content Automation Program
SOC	Secure Operations Center
SPF	Sender Policy Framework
SQL	Structured Query Language
SSD	Solid-state drive
SSL	Secure Sockets Layer
SW	Software
TIC	Trust Internet Connections
USB	Universal Serial Bus
US-CERT	United States Computer Emergency Readiness Team
USG	United States Government
USGCB	United States Government Configuration Baseline
VM	Virtual Machine
VPN	Virtual Private Network
WAN	Wide Area Network
WAP	Wireless Access Point

Appendix C: Mapping to NIST Controls

FY14 Metric	NIST Guidance	NIST Control (FIPS 200 Specs)
1.1. For each FIPS 199 impact level (H = High, M = Moderate, L = Low), what is the total number of information systems by organization (i.e., Bureau or Sub-Department Operating Element) categorized at that level? (Organizations with fewer than 5,000 users may report as one unit.)	NIST 800-53	CM-8, RA-2, PM-5
1.1.1. Organization-Operated Systems	NIST 800-53	CM-8,PM-5
1.1.2. Contractor-Operated Systems	NIST 800-53	CM-8, RA-2, PM-5
1.1.3. Systems (from 1.1.1 and 1.1.2) with Security ATO	NIST 800-53, NIST 800-37	CM-8, RA-2, PM-5
1.1.4. Systems (from 1.1.1 and 1.1.2) with expired Security ATO	NIST 800-53, NIST 800-37	CM-8, RA-2, PM-5
2.1. What is the total number of the organization's hardware assets connected to the organization's unclassified network(s)?	NIST 800-53	CM-8,PM-5
2.2. What percentage of assets in 2.1 are covered by an automated capability (scans/device discovery processes) to provide enterprise-level visibility into asset inventory information for all hardware assets?	NIST 800-53	CM-8 enhancement 2
2.2.1. What is the minimum frequency for device discovery scanning conducted on all assets?	NIST 800-53	CM-8 enhancement 3
2.3. Can the organization track the installed operating system's vendor, product, and version in use on the assets in 2.1?	NIST 800-53	CM-2
2.4. For what number of assets in 2.1 has the organization implemented an automated capability to detect and block unauthorized software from executing or for which no such software exists for the device type?	NIST 800-53	CM-2
3.1. For each operating system vendor, product, and version, combination referenced in 2.3, report the following:	NIST 800-53 NIST 800-70	

3.1.1. Has a minimal acceptable security configuration baseline been defined?	NIST 800-53	CM-2
3.1.2. How many hardware assets (which are covered by this baseline, if it exists) have this software?	NIST 800-53	CM-2
3.1.3. What is the percentage of the applicable hardware assets (per question 2.1) of each kind of operating system software in 3.1 that are covered by an automated capability to identify deviations from the approved configuration baselines identified in 3.1.1 and to provide visibility at the organization's enterprise level?	NIST 800-53	CM-2 enhancement 2, CM-6 control enhancement 1
4.1. What percentage of hardware assets identified in section 2.1 are evaluated using an automated capability that identifies NIST National Vulnerability Database vulnerabilities (CVEs) present with visibility at the organization's enterprise level?	NIST 800-53	SI-7
5.1. How many people have unprivileged network accounts? (Exclude privileged network accounts and non-user accounts.)	NIST 800-53,	IA-2
5.2. What percentage of people with an unprivileged network account can log onto the network in each of the following ways?	NIST 800-53	IA-2
5.2.1. Allowed to log on with user ID and password.	NIST 800-53	IA-2
5.2.2. Allowed, but not required, to log on with a non-PIV form of two-factor authentication.	NIST 800-53	IA-2 enhancement 2 and 7
5.2.3. Allowed, but not required, to log on with a two-factor PIV card.	NIST 800-53	IA-2 enhancement 2 and 7
5.2.4. Required to log on with a non-PIV form of two-factor authentication.	NIST 800-53	IA-2 enhancement 2 and 7
5.2.5. Required to log on with a two-factor PIV card.	NIST 800-53	IA-2 enhancement 2 and 7
5.2.6. Required to conduct PIV authentication at the user-account level.	NIST 800-53	IA-2 enhancement 2 and 7
5.3. How many people have privileged network accounts? (Exclude unprivileged network accounts and non-user accounts.)	NIST 800-53	IA-2 enhancements 3 and 6
5.4. What percentage of people with a privileged network account can log onto the network in each of the following ways?	NIST 800-53	IA-2
5.4.1. Allowed to log on with user ID and password.	NIST 800-	IA-2

	53	
5.4.2. Allowed, but not required, to log on with a non-PIV form of two-factor authentication.	NIST 800-53	IA-2 enhancements 1 and 6
5.4.3. Allowed, but not required, to log on with a two-factor PIV card.	NIST 800-53	IA-2 enhancements 1 and 6
5.4.4. Required to log on with a non-PIV form of two-factor authentication.	NIST 800-53	IA-2 enhancements 1 and 6
5.4.5. Required to log on with a two-factor PIV card.	NIST 800-53	IA-2 enhancements 1 and 6
5.4.6. Required to conduct PIV authentication at the user-account level.	NIST 800-53	IA-2 enhancements 1 and 6
5.5. How many people log onto the organization's remote access solution(s) to obtain access to the organization's desktop LAN/WAN resources or services?	NIST 800-53, NIST 800-63	AC-17
5.6. For remote access, what percentage of people can log onto the organization's desktop LAN/WAN resources or services in each of the following ways?	NIST 800-53, NIST 800-64	IA-2
5.6.1. Allowed to log on with user ID and password.	NIST 800-53, NIST 800-63	IA-2
5.6.2. Allowed, but not required, to log on with a non-PIV form of two-factor authentication.	NIST 800-53, NIST 800-64	IA-2
5.6.3. Allowed, but not required, to log on with a two-factor PIV card.	NIST 800-53, NIST 800-65	IA-2
5.6.4. Required to log on with a non-PIV form of two-factor authentication.	NIST 800-53, NIST 800-65	IA-2
5.6.5. Required to log on with a two-factor PIV card.	NIST 800-53, NIST 800-65	IA-2
5.6.6. Required to conduct PIV authentication at the user-account level.	NIST 800-53, NIST 800-65	IA-2

6.1. What is the estimated number of hardware assets from 2.1 in each of the following mobile asset types, and how many are encrypted?	NIST 800-53	AC-3
7.1. What percentage of external network traffic to/from the organization's networks passes through a TIC/MTIPS?	NIST 800-53	SC-7
7.2. What percentage of external network/application interconnections to/from the organization's networks passes through a TIC/MTIPS?	NIST 800-53	SC-7
7.3. What percentage of organization email systems implement sender verification (anti-spoofing) technologies when sending messages?	NIST 800-53	AU-10
7.4. What percentage of organization email systems use sender verification (anti-spoofing) technologies to detect possibly forged messages from outside the network?	NIST 800-53	AU-10
8.1. What percentage of the organization's network users have been given and successfully completed cybersecurity awareness training in the past year (at least annually)?	NIST 800-53	AT-2
8.1.1. What is the estimated percentage of new users who satisfactorily completed security awareness training before being granted network access, or completed security awareness training within an organizationally defined time limit that provides minimal acceptable security after being granted access?	NIST 800-53	AT-2

Table 6 – Mapping of FISMA Metrics to NIST Guidance and Controls